UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/614,487	07/11/2000	Eugene Amdur	DSC-003	2054

7733 7590 01/04/2005

WALKER & JOCKE, L.P.A.
231 SOUTH BROADWAY STREET
MEDINA, OH 44256

EXAMINER	
ADAMS, JONATHAN R	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 01/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/614,487	AMDUR ET AL.	
	Examiner	Art Unit	
	Jonathan R Adams	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 June 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *11-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-10 have been canceled.

2. Claims 11-16 have been amended

Response to Arguments

3. Applicant's arguments, see page 12, line 12, filed 6/21/04, with respect to the rejection(s) of claim(s) 11 under 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Devine et al., US Patent No 6606708.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claim 11 rejected under 35 U.S.C. 102(b) as being anticipated by Mitsutaka, Japanese Patent #11-98134-A(hereafter referred to as '134).

6. As to claim(s) 11:

'134 teaches a method for authenticating target data comprising:

- Client provides client-identifying data to one or more servers / Cookie transmitted to from user terminal to WWW service computer (Fig 2, Element 3, '134), provide identifying data is deemed to be inherent to the invention as disclosed above as "Cookies are used to Identify users" (Page 129, "cookie", Microsoft Computer Dictionary).
- Unique server identifier for each of server computers / www service adds digital signature to Cookie (Section 6, Line 3, '134)
- Request/Store public/private key from public key encryption system... / Efficient digital signature scheme (Section 19, Line 1, '134)
- Public key in database available to server computers and associate public key with unique server-identifier / public key must be available to server to validate digital signature, unique server-identifier (private key) is associated with public key by private/public key encryption/decryption relationship
- Server computers generate cookies for client computers / Cookie generation part at WWW service computer (Fig 1, Element 13, '134), cookie identification transmission to server (Fig 2, Element 3→3', '134)
- Cookie comprises client-identifying data provided by the client computers / "Cookies are used to Identify users" (Page 129, "cookie", Microsoft Computer Dictionary).
- Cookie comprises value of server-identifier assigned to the generating server / Adding digital signature to cookie (Section 6, Line 4 et seq., '134)

- Server generates encrypted digital signature for each cookie using private key / Digital signature combined with encryption of cookie (Section 6, Line 4 et seq., '134). Digital signatures undergo an encryption operation during processing.
- Servers forward cookies with encrypted digital signatures to client computers corresponding to identifying data provided / Cookies transmitted to client (Fig 2, '134)
- Server computers receive cookies with encrypted digital signatures from client computers / User terminal transmits encrypted message and digital signature to WWW service computer (Fig 2, '134)
- Servers extract server identifying data from received cookies to retrieve public keys to decrypt digital signatures and authenticate the cookies / Cookie verification part (Section 13, Line 6, '134)

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claim 12 rejected under 35 U.S.C. 103(a) as being unpatentable over '134.

As to claim(s) 12:

9. '134 teaches a method for authenticating target data by means of a public-key encryption system and storing the encryption key in memory. '134 does not explicitly teach the means to obtain a replacement key after a restart. The examiner takes official notice as to the means to obtain a replacement key after restart. It is well known in the art that many computer systems use a volatile dynamic memory as their primary memory, and so the key stored in memory would be erased upon restart. It would have been obvious to a person of ordinary skill in the art at the time of invention to obtain a replacement key on after restart. One of ordinary skill in the art would have been motivated to obtain a replacement key on after restart because the invention disclosed in '134 implemented on such a system would necessitate a means to obtain a replacement key after a restart.

10. Claim 13 rejected under 35 U.S.C. 103(a) as being unpatentable over '134 in view of Bruce Schneier, "Applied Cryptography".

11. '134 teaches a method for authenticating target data by means of a public-key encryption system. '134 does not teach all the specific key management techniques it employs, including the key lifecycle time. Schneier discloses some of the well known advantageous key lifecycle strategies:

- Determine an elapsed time... / There must be a policy that determines the permitted lifetime of a key (Page 184, Line 3 et seq., Schneier)

- Purge each public key... / old keys must be destroyed (Section 8.11, Line 1 et seq., Schneier)
- Longer than the elapsed time... / There must be a policy that determines the permitted lifetime of a key (Page 184, Line 3 et seq., Schneier)

It would have been obvious to a person of ordinary skill in the art at the time of invention to implement '134 with the key lifecycle strategies as disclosed in Schneier. One of ordinary skill in the art would have been motivated to implement these strategies because they are very well known in the art as advantageous security policies used on a variety of platforms.

12. Claim 13 rejected under 35 U.S.C. 103(a) as being unpatentable over '134 in view of Bruce Schneier, "Applied Cryptography", in further view of Devine et al., US Patent No 6606708 (hereafter referred to as '708).

13. As to claim(s) 14:

'134 teaches a client-server network authentication system comprising:

- Client provides client-identifying data to one or more servers / Cookie transmitted to from user terminal to WWW service computer (Fig 2, Element 3, '134), provide identifying data is deemed to be inherent to the invention as disclosed above as "Cookies are used to Identify users" (Page 129, "cookie", Microsoft Computer Dictionary).
- Unique server identifier for each of server computers / www service adds digital signature to Cookie (Section 6, Line 3, '134)

- Request/Store public/private key from public key encryption system... / Efficient digital signature scheme (Section 19, Line 1, '134)
- Public key in database available to server computers and associate public key with unique server-identifier / public key must be available to server to validate digital signature, unique server-identifier (private key) is associated with public key by private/public key encryption/decryption relationship
- Server computers generate cookies for client computers / Cookie generation part at WWW service computer (Fig 1, Element 13, '134), cookie identification transmission to server (Fig 2, Element 3→3', '134)
- Cookie comprises client-identifying data provided by the client computers / "Cookies are used to Identify users" (Page 129, "cookie", Microsoft Computer Dictionary).
- Cookie comprises value of server-identifier assigned to the generating server / Adding digital signature to cookie (Section 6, Line 4 et seq., '134)
- Server generates encrypted digital signature for each cookie using private key / Digital signature combined with encryption of cookie (Section 6, Line 4 et seq., '134). Digital signatures undergo an encryption operation during processing.
- Servers forward cookies with encrypted digital signatures to client computers corresponding to identifying data provided / Cookies transmitted to client (Fig 2, '134)

- Server computers receive cookies with encrypted digital signatures from client computers / User terminal transmits encrypted message and digital signature to WWW service computer (Fig 2, '134)
- Servers extract server identifying data from received cookies to retrieve public keys to decrypt digital signatures and authenticate the cookies / Cookie verification part (Section 13, Line 6, '134)

14. '134 does not specifically teach the use of multiple servers where the public key is stored in a database available to each one of the server computers. Schneier teaches the use of a centralized public key database for multiple parties to access the public key to a public/private key pair (Page 185,"Public-Key Key Management", Line 3 et seq., Schneier). It would have been obvious to a person of ordinary skill in the art at the time of invention to use the centralized public key database taught by Schneier in the invention of client-server system of '134. One of ordinary skill in the art would have been motivated to use the centralized public key database taught by Schneier in the invention of client-server system of '134 because the centralized public key database provides a simple scaleable public key management system.

15. '134 as modified above does not teach for the client to access a second server and for the second server to authenticate the client's cookie. '708 teaches a load balancing system for multiple servers to communicate with a client using authentication cookies (Col 23, Lines 29-33, '708), (Col 8, Lines 46-56, '708). It would have been obvious to a person of ordinary skill in the art at the time of invention to use the load balanced multiple server system of '708 with the invention of '134 as modified above.

One of ordinary skill in the art would have been motivated to use the load balanced multiple server system of '708 with the invention of '134 as modified above because the use of multiple servers allows for faster data communication speeds for a greater number of accessing clients.

16. As to claim(s) 15 and 16:

Claims 15 and 16 correspond to claims 12 and 13.

Conclusion

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jonathan R Adams whose telephone number is (571)272-3832. The examiner can normally be reached on Monday – Friday from 10am to 6pm.

18. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is (571)272-3838. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Andrew Caldwell
Andrew Caldwell